

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

UNITED STATES : CRIMINAL ACTION
v. : No. 08-26
REGINA TOLLIVER :

MEMORANDUM

Schiller, J.

January 25, 2010

Defendant Regina Tolliver, a former customer service representative at the King of Prussia Mall branch of Citizens Bank, moves this Court for judgment of acquittal or, alternatively, for a new trial following her convictions for bank fraud, aggravated identity theft, and unauthorized access of a financial record. At trial, Defendant did not dispute that the bank fraud occurred, but argued that someone else used her employee number and password to acquire the customer information that allowed this scheme to flourish.

In her post-trial motions, Defendant asserts that the Government's evidence is insufficient to sustain her guilt beyond a reasonable doubt. Defendant also argues that she is entitled to a new trial because her trial attorney was constitutionally ineffective. For the following reasons, Defendant's motions are denied.

I. BACKGROUND

Several false checks were cashed against the accounts of seven Citizens Bank customers between March and November of 2007. (Mar. 23, 2009 Tr. at 53-82; Gov't's Exs. 102, 103, 105-09, 111-12 [Sarah Migden False Checks] & Exs. 202-04A, 206-07 [Mary Renzi False Checks] & Exs. 302-04, 306-07, 309-11, 313-14 [Lisa Parise False Checks] & Exs. 402-03, 405-06 [Veronica Tucker

False Checks] & Exs 502-03, 505-06, 508, 510-11, 513, 515-16, 518, 520-21 [William Guzman False Checks] & Exs. 602-03, 605-06, 608-09 [Steven Mansh False Checks] & Exs. 702-09, 711-12, 714-16 [Evelyn Becker False Checks].) Images from Citizens Bank video cameras revealed that all of these checks were cashed by two “check runners,” a male and a female, posing as the Citizens Bank account holders. (Gov’t’s Exs. 101, 104, 107, 110, 201, 205, 301, 305, 308, 312, 401, 404, 501, 504, 507, 509, 512, 514, 517, 519, 601, 604, 607, 701, 710, 713 [Stills of Check Runners from Citizens Bank Video].)

All of these false checks were drawn on a bank other than Citizens Bank. Once the other banks refused to pay, the customers were charged the face value of the checks. (See Mar. 23, 2009 Tr. at 58-59; *see, e.g.*, Gov’t’s Ex. 102A [Returned Check with Stamp].) However, since the customers were ultimately determined to be victims of fraud, Citizens Bank credited their accounts for the full value of the loss. (Mar. 23, 2009 Tr. at 59.) The false checks amounted to \$181,577.00. (*Id.* at 82, 85-86; Gov’t’s Ex. 6 [Summ. of Fraudulent Transactions].) Thus, as a result of the fraud, Citizens Bank lost this amount. (See Mar. 23, 2009 Tr. at 61.)

At the time of the fraud, Citizens Bank utilized computer systems to manage and track its customer accounts. The systems contained personal information, including names, addresses, dates of birth, social security numbers, driver’s license numbers, Citizens Bank account numbers, and the amount of money in those accounts. (*Id.* at 31.) Bank employees could access this information through two systems — the main frame system and the touch point system — by entering their employee number and password.¹ (*Id.* at 31-33, 125.)

¹ An employee might check both systems because, occasionally, the main frame system contained information that was not in the touch point system. (Mar. 23, 2009 Tr. at 157-58.) The account information in this case was mainly accessed via the touch point system, but was

Each Citizens Bank employee is assigned an employee number, which is not confidential. (*Id.* at 124.) The individual employees then select a password. (*Id.* at 33.) Citizens Bank employees are instructed that their password must be kept secure and confidential and should not be written down. (*Id.* at 34; Mar. 24, 2009 Tr. at 24, 29, 33, 37-38, 43-44, 59-60.) Employees are not permitted to share their passwords with anyone else, including other Citizens Bank employees. (Mar. 23, 2009 Tr. at 34, 155.) If an employee believes that another person has learned his or her password, the employee is required to inform management and change the password immediately. (*Id.* at 34, 155-56.) If an employee must leave a terminal that she has signed into, even if just to go to the bathroom, the employee is required to temporarily lock the terminal or sign off completely. (*Id.* at 156.) Employees use their passwords frequently, between ten and fifty times daily. (Mar. 24, 2009 Tr. at 24, 30, 34, 38, 44, 60.) Additionally, Citizens Bank employees are required to change their password every two to three months. (Mar. 23, 2009 Tr. at 33.)

When a Citizens Bank employee accesses either system, data concerning that activity is archived into an employee tracking system for six months. (*Id.* at 36.) This data can be recalled to determine the employee number and password entered to access certain accounts. (*Id.*) This is known as the employee's "footprint." (*Id.*)

As part of his investigation in this case, Todd Swoyer, the fraud investigator at Citizens Bank assigned to this case, ran a footprint report for each of the accounts that had been compromised. (*Id.* at 87.) Swoyer's investigation revealed that Defendant's employee number was the only one that had been used to access all seven of these individuals' account information. (*Id.* at 121; Gov't's Exs. 4, 5, 114, 209, 316, 410, 531, 614, 616, 718 [Swoyer's Footprint Searches].) Swoyer's searches also

also accessed via the main frame system.

revealed that, with one exception, after Defendant's username and password were entered to look up the account information, someone called the Citizens Bank automated system to check the balances of those accounts either shortly after the accounts were accessed or shortly before the fraudulent checks were cashed against the accounts. (Mar. 23, 2009 Tr. at 94-95; Gov't's Exs. 114, 209, 316, 410, 531, 614, 616, 718.) All of the victims who testified stated that they had not made those calls. (Mar. 23, 2009 Tr. at 214; Mar. 24, 2009 Tr. at 11, 19-21, 65.)

The Citizens Bank branch at the King of Prussia Mall maintained several universal computer terminals, which any employee could log onto using his or her employee number and password. (*Id.* at 144.) Swoyer's investigation revealed that the seven customers' accounts were accessed under Defendant's employee number on February 5th and 8th of 2007 and on March 7th, 8th, and 9th of 2007. The Citizens Bank information technology service was able to determine that the first accounts that were hit were accessed from the King of Prussia Mall branch, where Defendant worked. (*Id.* at 118; Mar. 24, 2009 Tr. at 49; Gov't's Ex. 2 [Spreadsheet] & Ex. 10 [Employee Schedule].) Defendant's employee number was in use at three different terminals at the same time on at least one of those days. (Mar. 23, 2009 Tr. at 133; Mar. 24, 2009 Tr. at 51-53.) However, it was not uncommon for an employee to be logged into multiple terminals at once. (Mar. 23, 2009 Tr. at 157.)

Employee schedules and time and attendance records confirmed that Defendant worked on all of the days that her password was used to access the victims' accounts. (Employee Schedule & Gov't's Ex. 10A [Time and Attendance Records].) Defendant's employee log book for those dates reflected that she had not contacted any of the seven victims for sales or business purposes. (Mar. 23, 2009 Tr. at 160, 163; Gov't's Ex. 12A [Def.'s Log Book].) Nor was Defendant assigned to contact any of these individuals for sales purposes. (Mar. 23, 2009 Tr. at 173-74.) Palma Salvucci,

the branch manager in 2007, testified that Citizens Bank employees would not be permitted to look at a customer's account and personal information for a reason other than one related to Citizens Bank's business. (*Id.* at 165.)

According to the schedules, the only employees other than Tolliver at the King of Prussia Mall branch who arguably worked on the relevant days were Angela Anderson and Debby Clarke. Clarke was initially marked as "OFF" for February 8th, March 7th, and March 8th, but the notation "KOP" was written next to her slot on those dates. Salvucci, who assembled the schedules, testified that she used this notation when asked to lend an employee for the day to the other Citizens Bank branch in King of Prussia and that she would change it if she received a call not to send the employee. (*Id.* at 152.) However, she testified that it is not possible to know for sure, based only on the schedule, whether an individual marked as working at the other Citizens Bank branch for the day in fact did so. (*Id.* at 153.) Indeed, although the "KOP" notation appeared next to Clarke's schedule for March 7th and 8th, the time and attendance records reflect that she did not work at all on those days.² (Gov't's Ex. 10A.)

Swoyer and Postal Inspector Frank Busch interviewed Defendant on March 15, 2007. (Mar. 23, 2009 Tr. at 122, 196.) Defendant told Swoyer that she had not given her password to anyone, and stated that she always locked her computer when she walked away from a terminal. (*Id.* at 122) Additionally, all of Defendant's former co-workers who testified at trial claimed that they never knew Defendant's password and that they never saw her password written down. (*Id.* at 156; Mar.

² The "KOP" notation was written on Defendant's schedule for February 8, 2007. (Gov't's Ex. 10.) The time and attendance records reflect that, whether she worked at the King of Prussia Mall branch or the other Citizens Bank branch in King of Prussia, Defendant worked on that day. (Gov't's Ex. 10A.) There was no evidence at trial identifying the branch that the victims' accounts were accessed on February 8, 2007.

24, 2009 Tr. at 25, 30-31, 34-35, 39, 44-45, 60.) Although a page in Defendant's log book read "password, Aries12, as HR express, password, evillass, lifecare, RSM1love, Aries12," Defendant told Swoyer that these were not her passwords to access the touch point or the main frame systems. (Mar. 23, 2009 Tr. at 137.) Defendant was terminated that day. (*Id.* at 131.)

The Government theorized that Defendant accessed customers' personal and account information and passed this information along for use in a scheme to defraud Citizens Bank. Ultimately, the information was used to create false identification documents, which were used by the check runners to cash fraudulent checks against the targeted accounts. However, neither of the check runners in this case, both of whom had been arrested, implicated Defendant. (*Id.* at 198.)

At trial, the Court admitted Inspector Busch as an expert in the area of bank fraud investigation. (*Id.* at 175.) Busch, the Government's expert on financial crimes, testified about the structure of bank fraud schemes generally, based on his 14 ½ years of experience investigating financial crimes for the United States Postal Inspection Service. (*Id.* at 175-77.) He has received extensive training in investigating criminal financial crimes. (*Id.* at 175.) He has completed approximately 1,000 fraud and identity theft investigations, acting mainly as lead investigator in those matters. (*Id.* at 176.) His experience includes hundreds of bank fraud/identity theft cases in Philadelphia. (*Id.* at 177.)

Inspector Busch testified that bank fraud schemes generally involve the following participants: a ring leader who heads the operation; a second in command who, among other things, recruits individuals to assist in the operation; individuals who can access or create counterfeit documents; drivers who take check runners to the bank to cash the false checks; check runners who go into the bank to cash the checks; and individuals, such as employees at banks or insurance

companies, who access personal information to be used in the scheme. (*Id.* at 178, 182, 187.) According to Inspector Busch, the bank employee would typically be in touch with the ring leader of the operation or the middle man who recruited her, but would not have contact with the check runners. (*Id.* at 179-81.) Thus, in his experience, check runners generally do not know the identity of the person who is obtaining the information necessary to facilitate the crime. (*Id.* at 183-84.)

Inspector Busch also explained that, in general, a bank employee will access personal information, write it down or print it out, and then pass it along to be used in the scheme. (*Id.* at 189.) It is common, he testified, for someone in the scheme to call the automated system to confirm that the targeted accounts are active and functioning properly. (*Id.* at 190.)

Following her conviction, Tolliver filed her first motion for acquittal or in the alternative for a new trial on July 6, 2009. The Court denied her motion on July 29, 2009. In arguing for acquittal, Tolliver did not dispute that a bank fraud occurred, but argued that the Government failed to prove beyond a reasonable doubt that she was the person who used her password to access the customer accounts. The Court found that based on the above described evidence, “a reasonable jury could infer that only Defendant knew her password and that it was she who input her password into the system.” (Ct.’s July 29, 2009 Mem. at 10.) Therefore, the Court held that a reasonable jury could conclude that the Government proved its case beyond a reasonable doubt and denied Defendant’s motion for a judgment of acquittal. (*Id.* at 13-14.) Tolliver alternatively moved for a new trial on the grounds that “the Government focused on ‘the defendant’s lack of a[n] explanation or evidence’ to prove its case, thereby ‘violat[ing] the defendant’s constitutional right to remain silent and unconstitutionally shift[ing] the burden of proof upon defendant.’” (*Id.* at 14.) The Court found that no constitutional violation had taken place, and denied Tolliver’s motion for a new trial. (*Id.* at 14-

15.)

On September 4, 2009, the Court granted Defendant's Motion for Leave to File Motion for Reconsideration Out of Time and Supplemental Post-Trial Motions. The instant motion followed.

II. STANDARD OF REVIEW

Pursuant to Federal Rule of Criminal Procedure 33, a court may grant a new trial "if the interest of justice so requires." FED. R. CRIM. P. 33(a). A district court may, in its discretion, "grant a defendant a new trial only if it finds that 'there is a serious danger that a miscarriage of justice has occurred—that is, that an innocent person has been convicted.'" *United States v. Rich*, 326 F. Supp. 2d 670, 673 (E.D. Pa. 2004) (quoting *United States v. Johnson*, 302 F.3d 139, 150 (3d Cir. 2002)). A court may also grant a new trial "if errors occurred during the trial, and it is reasonably possible that such an error, or combination of errors, substantially influenced the jury's decision." *Id.* (citing *United States v. Copple*, 24 F.3d 535, 547 n.17 (3d Cir. 1994)). Although this standard is broader than the standard for acquittal under Rule 29, motions for a new trial are disfavored and "only granted with great caution and at the discretion of the trial court." *United States v. Martinez*, 69 F. App'x 513, 516 (3d Cir. 2003).

When considering a motion for judgment of acquittal premised on a claim that the evidence at trial was insufficient to support a conviction pursuant to Federal Rule of Criminal Procedure 29, a district court views the evidence "in the light most favorable to the government and affirm[s] the judgment if there is substantial evidence from which any rational trier of fact could find [the defendant] guilt[y] beyond a reasonable doubt." *United States v. Frorup*, 963 F.2d 41, 42 (3d Cir. 1992); *see also United States v. Gambone*, 314 F.3d 163, 170 (3d Cir. 2003); FED. R. CRIM. P. 29.

A court must “credit all available inferences in favor of the government.” *United States v. Riddick*, 156 F.3d 505, 509 (3d Cir. 1998). If evidence emerges from the trial that supports the jury’s verdict, regardless of how probative the court believes it to be, then a defendant’s motion for acquittal based on insufficient evidence should be denied. *See United States v. McNeill*, 887 F.2d 448, 450 (3d Cir. 1989). “The ‘contention that the evidence also permits a less sinister conclusion is immaterial. To sustain the jury’s verdict, the evidence does not need to be inconsistent with every conclusion save that of guilt.’” *United States v. Smith*, 294 F.3d 473, 478 (3d Cir. 2002) (quoting *United States v. Dent*, 149 F.3d 180, 188 (3d Cir. 1998)).

III. DISCUSSION

A. Defendant is not Entitled to a New Trial

Defendant asserts that she is entitled to a new trial because her trial counsel’s performance was constitutionally ineffective due to the fact that he did not object to the expert testimony of Inspector Busch.³ Defendant claims that objections should have been made to the qualification of

³ As a preliminary matter, the Court recognizes that Sixth Amendment ineffective assistance of counsel claims are not generally entertained in a motion for a new trial, but rather through collateral proceedings. *See United States v. Washington*, Crim. A. No. 08-4181, 2009 WL 4827496, at *3 (3d Cir. Dec. 16, 2009). However, there is support for the jurisdiction of district courts to entertain certain ineffective assistance of counsel claims through a motion for a new trial. *United States v. Cronic*, 466 U.S. 648 n.42 (1984) (“The District Court had jurisdiction to entertain the motion [for new trial based on ineffective assistance of counsel] and either deny the motion on its merits, or certify its intention to grant the motion to the Court of Appeals, which could then entertain a motion to remand the case.”). Entertaining such a motion is proper if the record is sufficient for a determination on the issue. *Washington*, 2009 WL 4827496, at *3. In this case, the Government waived objection to the Court entertaining this motion, agreeing that the Court has jurisdiction to do so. (Gov’t’s Resp. in Opp’n to Def.’s Mot. For Acquittal at 21.) The Court deems the record sufficient to determine the motion, and it is in the interest of judicial economy to do so.

Busch as an expert, as well as to seven specific pieces of his testimony. The Court disagrees that counsel's performance was rendered ineffective due to his decision not to object to Busch's testimony or admission as an expert.

To establish ineffective assistance of counsel, one "must prove both incompetence and prejudice." *Kimmelman v. Morrison*, 477 U.S. 365, 381 (1986) (citing *Strickland v. Washington*, 466 U.S. 668, 687 (1984)). To satisfy the first prong, a defendant must prove that counsel's performance was deficient, meaning that counsel committed errors so serious, that he failed to function as "counsel" guaranteed by the Sixth Amendment. *Strickland*, 466 U.S. at 687. To meet the second prong, a defendant must show that there is a "reasonable probability that, but for counsel's unprofessional errors, the result of the proceedings would have been different." *Id.* at 694. A reasonable probability is a probability sufficient to undermine confidence in the outcome. *Id.* The Court must defer to strategic decisions of counsel, and provide deference to counsel's trial performance. *Id.* at 689.

Counsel's performance was within the "wide range of reasonable professional assistance," and was therefore not deficient. *Id.* at 689. While counsel could have raised the objections that Defendant now suggests, he was not obligated to do so. It is not the Court's role to second guess an attorney's strategic decisions. Counsel decided not to object to Busch testifying as a expert, in order to use cross-examination to elicit specific testimony from Busch. (Mar. 23, 2009 Tr. at 177, 191-200.) On cross-examination, counsel attempted to elicit testimony that would indicate that Tolliver was not the perpetrator. Counsel asked questions about whether a bank insider would use someone else's employee ID numbers and passwords, and whether ring leaders would instruct them to do so. (*Id.* at 192-94.) He attempted to elicit testimony that bank insiders with no criminal records would

generally turn on the ring leaders in order to protect themselves from criminal liability. (*Id.* at 194-95.) He asked Busch about the check runners in this case in order to draw out the fact that both have pled guilty, but did not implicate Tolliver as involved in their crime. (*Id.* at 197-98.) He asked about evidence as to Tolliver’s connection to the crimes. (*Id.* at 198.) He elicited testimony that there was no unusual activity on Tolliver’s personal bank accounts. (*Id.* at 198.) He asked if phone records existed that showed that she had contacted or been contacted by any “bad guys.” (*Id.* at 199.) On cross, Busch conceded that there was no surveillance evidence linking Tolliver to the crime. (*Id.* at 200.) In order to counter Busch’s testimony that people involved in bank fraud schemes frequently change phones, counsel attempted to elicit testimony that Tolliver only has one cell phone and has not switched her number. (*Id.* at 191-192.)

The theories and strategies of reasonable attorneys will differ. While many attorneys may have made the objections that Defendant now suggests, trial counsel made a strategic decision not to object to Busch’s expert status or to keep him from testifying about the general profile of the scheme, but to elicit testimony on cross-examination that demonstrated the ways in which Tolliver did not fit that profile. This was reasonable, and certainly within the wide range of professionally acceptable behavior.

Regardless, Defendant was not prejudiced. To be prejudiced for purposes of an ineffectiveness claim, there must be a reasonable probability that but for counsel’s errors, Tolliver would not have been convicted. *See Strickland*, 466 U.S. at 694. Tolliver cannot support this contention. As was fully discussed in this Court’s July 29, 2009 Memorandum, the Government produced sufficient evidence to uphold Tolliver’s convictions. Even without Busch’s testimony, a reasonable jury could have convicted Tolliver.

The Government unquestionably established that false checks in the amount of \$181,577.00 were cashed against the accounts of seven Citizens Bank customers as part of a scheme to defraud Citizens Bank and that Citizens Bank sustained a loss in that amount. The Government also established that someone used Defendant's employee number and password to access the account and personal information of these seven individuals and that Defendant's employee number was the only employee number used in relation to all seven accounts. The close temporal proximity between the accessing of the accounts and the inquiries into the Citizens Bank automated system, along with the subsequent cashing of false checks supports the conclusion that someone used Defendant's employee number and password with the intent to further the scheme to defraud the bank. The Government provided circumstantial evidence that it was Defendant, and not another person using Defendant's password, who accessed the account information. Evidence at trial showed that Citizens Bank employees select their own passwords, are instructed to keep their passwords secret and are prohibited from sharing them with other employees or writing them down. Defendant herself told Mr. Swoyer and Inspector Busch that she safeguarded her password and that she had not given it to anyone else. Furthermore, all of Defendant's former co-workers who testified at trial stated that they did not know Defendant's password. There was also evidence that Defendant worked on each of the days that the victims' accounts were accessed with her password and evidence that there was no legitimate business purpose for her to access those accounts. Based on this evidence, a reasonable jury could infer that only Defendant knew her password and that it was she who input her password into the system.

Defendant also argues for a new trial on the grounds that the Court committed plain error by deciding not to exclude Inspector Busch's testimony *sua sponte*. A district court has broad discretion

in deciding whether to admit expert testimony. *See U.S. v. Brink*, 39 F.3d 419, 427 n.13 (3d Cir. 1994); *Fuentes v. Reilly*, 590 F.2d 509, 511 (3d Cir. 1979). Here, the court followed the accepted practice of allowing a law enforcement expert to testify concerning the methods and practices generally employed in a particular area of criminal activity. *See e.g. United States v. Gibbs*, 190 F.3d 188, 211 (3d Cir. 1999) (noting that it is well established that experienced government agents may testify to the meaning of coded drug language); *United States v. Pungitore*, 910 F.2d 1084, 1149 (3d Cir. 1990) (upholding admission of expert to testify as to the structure of crime families and interplay of them on a national level); *United States v. Robertson*, 387 F.3d 702, 704 (8th Cir. 2004) (expert testified as to typical behavior of individuals involved in drug trafficking); *United States v. Locascio*, 6 F.3d 924, 936-37 (2d Cir. 1993) (upholding admission of agent testimony that explained the operation, structure, membership, and terminology of organized crime families). Busch was admitted as an expert in the area of bank fraud investigation. His testimony assisted the jury in understanding bank fraud schemes. As was previously discussed, defense counsel employed a strategy whereby he allowed Busch to be admitted as an expert without objection so that he would have the opportunity to cross-examine him. The Court treads very lightly on the strategy of counsel during the course of trial, except as to opine as to reasonableness, as was previously expounded upon. The Court finds no miscarriage of justice or plain error in this decision. Accordingly, a new trial is not warranted.

B. Defendant is Not Entitled to Judgment of Acquittal

On July 29, 2009 the Court denied Defendant's first Motion for Acquittal. In that motion Defendant argued that the Government had produced insufficient evidence to prove the elements of the crimes of which she was convicted. In the instant motion, Defendant again challenges the

sufficiency of the evidence against her. The present motion is in substance, a motion for reconsideration. A proper motion for reconsideration serves to correct manifest errors of law or fact or to present newly discovered evidence. *Max's Seafood Café v. Quinteros*, 176 F.3d 669, 677 (3d Cir. 1999) (citing *North River Ins. Co. v. CIGNA Reinsurance Co.*, 52 F.3d 1194, 1218 (3d Cir. 1995)). Such a motion may be granted only if: 1) there has been an intervening change in the controlling law; 2) new evidence has recently become available; or 3) it is necessary to correct a clear error of law or to prevent manifest injustice. *Drysdale v. Woerth*, 153 F. Supp. 2d 678, 682 (E.D. Pa. 2001) (citing *United Lawnmower Sales & Service, Inc. v. Hagel*, Civ. A. No. 95-6157, 1997 WL 327564 at *2 (E.D. Pa. June 12, 1997)). A motion for reconsideration is not to be used as a means to reargue matters already argued and disposed of. *Drysdale*, 153 F. Supp. 2d at 682 (citing *Moyer v. Italwork*, Civ. A. No. 95-2264, 1997 WL 312178 at *3 (E.D. Pa. June 3, 1997)). Motions for reconsideration are to be granted sparingly. *Cont. Cas. Co. v. Diversified Indus.*, 884 F.Supp. 937, 943 (E.D. Pa. 1995).

The Court has previously ruled that the Government proved its case beyond a reasonable doubt and therefore denied Defendant's motion for a judgment of acquittal. Nothing has changed since the Court last considered this argument by Defendant. The law has not changed, no newly discovered facts have been alleged, and nothing has occurred that would make the Court reverse its previous decision that no clear error or manifest injustice has occurred. Defendant simply repackages her argument that the Government produced insufficient evidence to support her convictions. Accordingly, the Court denies Defendant's motion for acquittal.

IV. CONCLUSION

Defendant's trial counsel was not constitutionally ineffective. Defendant's motion for a new trial is denied. Defendant's motion for judgment of acquittal is denied because there is nothing that warrants reconsideration of that issue. An appropriate Order will be docketed separately.